**Amendments to the Claims:**

This listing of claims will replace all prior versions, and listings of claims in the application:

**Listing of Claims:**

1.-8. (Canceled)

9. (Currently amended) A computer-implemented method for ensuring non-repudiation of a payment request, the payment request being generated in a computing environment having a connection to a network, the method comprising the steps of:

receiving, over the network, the payment request together with a certificate identifying a user having caused the payment request to be generated, the certificate including certificate-identifying information and user-identifying information, the certificate further including authority information defining an authority of the user to make the payment request, the authority information including a maximum payment that the user is authorized to make and an identification of payees to whom the user is authorized to make payments;

validating the certificate-identifying information and the user-identifying information included within the received certificate;

accessing a store of authority information that is coupled to the network, that is stored apart from the payment request and that is independent of the received certificate;

retrieving, from the accessed store of authority information, stored authority information that is associated with the user;

comparing the retrieved authority information with the authority information included within the received certificate to determine whether the retrieved authority information matches the authority information included within the received certificate;

validating the authority information within the received certificate only if the retrieved authority information matches the authority information included within the received certificate, and

executing of the payment request only when the certificate-identifying information, the user-identifying information and the authority information within the received certificate is successfully validated.

10. (Original) The method of claim 9, wherein the payment request is for a predetermined amount and wherein the payment request is authorized only when the validating steps are successful and when the authority information for the user stored in the hierarchical authority data structure lists an authorized amount for the user at least equal to the predetermined amount.

11. (Original) The method of claim 9, wherein the certificate received in the receiving step conforms to the X.509 standard.

12. (Original) The method of claim 9, wherein the authority information is configured as XML code.

13. (Original) The method of claim 9, wherein the XML code is compliant with a DSML standard.

14. (Canceled)

15. (Currently amended) A computer-readable storage medium configured to store one or more software application configured to carry out a financial transaction, the application being configured to run on a computer coupled to a network, ~~and comprising, stored on a~~ the computer-readable storage medium comprising:

certificate receiving code which is configured to receive a digital certificate from a user over the network, the certificate including certificate-identifying information and user-identifying information, the certificate further including authority information that defines an authority granted to the user to request that the financial transaction be carried out, the authority information including a maximum payment that the user is authorized to make and an identification of payees to whom the user is authorized to make payments;

certificate validating code configured to enable validation of the certificate-identifying information and user-identifying information within the received certificate, and

authorization validating code configured to cause the computer to carry out steps of:

accessing a store of authority information that is coupled to the network, that is stored apart from the payment request and that is independent of the received certificate;

retrieving, from the accessed data structure, stored authority information that is associated with the user;

comparing the retrieved authority information with the authority information included within the received certificate to determine whether the retrieved authority information matches the authority information included within the received certificate;

validating the authority information within the received certificate only if the retrieved authority information matches the authority information included within the received certificate, and

executing of the financial transaction only when the authority information within the received certificate is successfully validated.

16. (Currently amended) The computer-readable storage medium ~~software application~~ of claim 15, wherein the digital certificate conforms to the X.509 standard.

17. (Currently amended) The computer-readable storage medium ~~software application~~ of claim 15, wherein the authority information is configured as XML code.

18. (Currently amended) The computer-readable storage medium ~~software application~~ of claim 17, wherein the XML code is compliant with a DSML standard.

19. (Currently amended) The computer-readable storage medium ~~software application~~ of claim 15, wherein the authority defined by the authority information within the received certificate also defines rights of the user to access predetermined data and programs within the network.

20.-28. (Canceled)

29. (Currently amended) ~~In a computing environment having a connection to a network, computer readable code readable by a computer system in said environment, for enabling a~~ A server computer ~~within the computing environment~~ to ~~both~~ authenticate a user of a client computer ~~within the computing environment~~ and to verify that the user is authorized to request that the server computer carry out a requested action, the server computer comprising:

a processor; and

a memory coupled to the processor and configured to store a set of instructions that when executed by the processor causes the processor to:

receive a payment request along with a digital certificate assigned to the user of the client computer, the digital certificate comprising a first code portion and a second code portion,

wherein the first code portion of the digital certificate is configured to enable authentication of the user, the first code portion defines a public key, a certificate serial number, a certificate validity period, a digital signature of the certificate authority, and an extension field,

wherein the second code portion of the digital certificate is configured to define an authority of the user of the client computer to request that the server computer carry out the requested action, the second code portion being configured for inclusion within the extension field of the first code portion, the authority of the user defined within the second code portion of the certificate defining access rights of the user including a maximum payment that the user is authorized to make and an identification of payees to whom the user is authorized to make payments ~~to data and programs within the computing environment;~~[[,]] ~~and code for causing the server computer to carry out steps of:~~

access[[ing]] a store of authority information that is coupled to the network, that is stored ~~apart from the payment request and that is~~ independent of the received digital certificate;

retrieve[[ing]], from the accessed store of authority information, authority information that is associated with the user of the client computer;

compare[[ing]] the retrieved authority information with the authority information included within the digital certificate to determine whether the retrieved authority information matches the authority information included within the digital certificate;

validate[[ing]] the authority information within the digital certificate only if the retrieved authority information matches the authority information included within the digital certificate, and

carry[[ing]] out the requested action only when the authority information within the digital certificate is successfully validated.

30. (Currently amended) The server computer ~~readable code~~ of claim 29, wherein the digital certificate conforms to the X.509 standard.

31. (Currently amended) The server computer ~~readable code~~ of claim 2.9, wherein the second code portion is configured as XML code.

32. (Currently amended) The server computer ~~readable code~~ of claim 31, wherein the XML code is compliant with a DSML standard.

33. (Currently amended) The server computer ~~readable code~~ of claim 29, wherein the authority of the user of the client computer is stored in a hierarchical authority data structure that is accessible by the server computer.